



# Протокол интеграции WebDel

Редакция от 13.09.2023.

## Оглавление

1.	Введение .....	3
2.	Общее описание порядка взаимодействия .....	4
3.	Настройка на стороне «Sigur» .....	5
4.	Протокол обмена .....	8
4.1.	Делегирование .....	8
4.2.	Доставка проходов .....	12
5.	Контакты .....	14

# 1. Введение

Данный документ описывает возможности СКУД «Sigur» (далее система) по делегированию внешнему веб-сервису решений о предоставлении доступа.

Функционал делегирования в описанном виде соответствует версии ПО «Sigur» 1.1.1.51.

## **2. Общее описание порядка взаимодействия**

Взаимодействие выполняется HTTP(S) POST-запросами, исходящими от сервиса «Sigur» (служба Windows либо демон Linux, осуществляющая взаимодействие с оборудованием).

Получателем запросов является внешняя система.

Данные передаются в формате JSON в кодировке UTF-8. Исходящие от «Sigur» данные передаются в теле POST-запроса, информация от внешней системы передается в данных ответа на HTTP(S)-запрос.

Система поддерживает работу по протоколам HTTP и HTTPS.  
Поддерживается HTTP-аутентификация.

Система поддерживает отправку HTTP-запросов как напрямую, так и через HTTP-прокси. Поддерживаются прокси как с аутентификацией, так и без неё.

### 3. Настройка на стороне «Sigur»

Для активации функционала необходимо:

1. Добавить в систему реквизиты соединения с внешним сервисом.

Для этого нужно перейти в меню «Файл» - «Настройки» - «WEB-делегирование» ПО «Клиент» и заполнить поля:

- URL делегирования. Адрес сервиса, принимающего решения о предоставлении доступа.
- URL доставки проходов. Адрес сервиса, принимающего события совершённых проходов.
- Использовать аутентификацию. Признак необходимости использования HTTP-аутентификации при запросах к URL.
- Логин. Логин для HTTP-аутентификации.
- Пароль. Пароль для HTTP-аутентификации.

URL-адреса указываются с префиксом «http://» или «https://». Любой из двух URL может быть не задан (пуст), тогда соответствующий сервис не будет использоваться.

Редактирование настроек
×

Наблюдение	URL делегирования:	<input type="text" value="http://test.com/delegation.php"/>
1С:Предприятие	URL доставки проходов:	<input type="text" value="http://test.com/events.php"/>
Видеонаблюдение	<input type="checkbox"/> Делегировать только запросы по неизвестным картам	
Печать пропусков	<input checked="" type="checkbox"/> Использовать аутентификацию	
Платёжная система	Логин:	<input type="text" value="user"/>
SMS	Пароль:	<input type="password" value="....."/>
Telegram		
E-Mail		
Персонал		
Бесконтактная идентификация		
Биометрика		
Распознавание лиц		
Active Directory		
Оправдательные документы		
Пропуска посетителей		
Архив		
Синхронизация данных		
Распознавание документов		
Беспроводные замки		
Устройства хранения		
Зоны		
Повторные проходы		
Дополнительные параметры		
HTTP (WEB)		
Заявки		
<b>WEB-делегирование</b>		
Права операторов		
BAS-IP		
True IP		
Профили шифрования OSDP		
Индикация		
Профили шифрования		

OK
Отмена

Окно «WEB-делегирование».

При необходимости отправки запросов через HTTP-прокси перейдите на вкладку «Файл» - «Настройки» - «HTTP (WEB)», установите галочку «Использовать прокси» и укажите IP-адрес прокси-сервера и порт.

Дополнительно Вы можете включить опцию «Прокси требует аутентификации», после чего ввести логин и пароль для доступа.

is Редактирование настроек

Наблюдение
1С:Предприятие
Видеонаблюдение
Печать пропусков
Платежная система
SMS
Telegram
E-Mail
Персонал
Бесконтактная идентификация
Биометрика
Распознавание лиц
Active Directory
Оправдательные документы
Пропуска посетителей
Архив
Синхронизация данных
Распознавание документов
Беспроводные замки
Устройства хранения
Зоны
Повторные проходы
Дополнительные параметры
<b>HTTP (WEB)</b>
Заявки
WEB-делегирование
Права операторов
BAS-IP
True IP
Профили шифрования OSDP
Индикация
Профили шифрования

☒ Использовать прокси

IP-адрес:

Порт:

☒ Прокси требует аутентификации

Логин:

Пароль:

OK Отмена

Настройки HTTP-прокси.






2. Включить функцию делегирования контроллером принятия решений серверу «Sigur».

Для этого необходимо перейти на вкладку «Оборудование» ПО «Клиент», выбрать в списке оборудования точку доступа на необходимом контроллере и нажать кнопку «Настройки».

Далее нужно перейти на вкладку «Общее», снять галочку «Отображать только базовые настройки» и выбрать в выпадающем списке «Делегировать серверу принятие решения» вариант «Да, все запросы» или «Да, только запросы по неизвестным пропускам».

По умолчанию контроллеры «Sigur» принимают решения автономно и не обращаются к сервису системы.

is Редактирование настроек

Конфигурация: (Пользовательская)
 





Общее
 Точка доступа 1
 Точка доступа 2
 Точка доступа 3
 Точка доступа 4

Вход сброса кол-ва людей в зоне  
 Не выбран

Линия индикации LED3 считывателя 1  
 Не выбран

Линия индикации LED3 считывателя 2  
 Не выбран

Линия индикации LED3 считывателя 3  
 Не выбран

Линия индикации LED3 считывателя 4  
 Не выбран

Время ожидания санкции оператора на доступ  
 < 10,00 с.

Делегировать серверу принятие решения:  
 да, все запросы

Управление индикацией считывателей

LED1 LED2 LED3

☒ Сигнализировать о разрешении доступа  
 короткий сигналом

☒ Сигнализировать о запрете доступа (три коротких сигнала)

☐ Сигнализировать о состоянии точки доступа  
 если точка в "нормальной" режиме

☒ Сигнализировать другие ситуации (удержание двери, ожидание PIN и пр.)

☐ Инвертировать результирующий сигнал

☐ Не проверять контрольную сумму Wiegand

☐ Игнорировать facility часть номеров пропусков

☐ Отображать только базовые настройки

OK Отмена

Активация функции «Делегировать серверу принятие решения».

## 4. Протокол обмена

### 4.1. Делегирование

Если в настройках задан URL делегирования, то по факту идентификации сотрудника система выполнит HTTP(S) POST-запрос по указанному URL.

Пример данных, которые будут переданы в теле запроса внешней системе при идентификации сотрудника считывателем, подключенным к контроллеру СКУД:

```
{
  "type": "NORMAL",
  "keyHex": "5AB860",
  "direction": 2,
  "accessPoint": 1
}
```

Пример данных, которые будут переданы в теле запроса при распознавании гос. номера автомобиля одной из интегрированных в «Sigur» систем видеонаблюдения:

```
{
  "type": "NORMAL",
  "lpNumber": "A123AA12",
  "direction": 2,
  "accessPoint": 1
}
```

Пример данных, которые будут переданы в теле запроса при распознавании лица одной из интегрированных в «Sigur» систем видеонаблюдения или самим сервером «Sigur»:

```
{
  "type": "NORMAL",
  "empid": "12",
  "direction": 2,
  "accessPoint": 1
}
```



### Содержимое тела HTTP POST-запроса по URL делегирования.

Параметр	Значение
type	В описываемой ситуации всегда имеет значение «NORMAL». Другие значения соответствуют специальным логикам доступа, таким как «доступ в сопровождении» и др.
keyHex	Номер идентификатора, принятого от считывателя на контроллер. Передается в шестнадцатеричном виде, может иметь различную длину – от 3 до 7 байт. Длина определяется тем, сколько данных считыватель присылает на контроллер. Так, 3 байта соответствуют протоколу Wiegand-26, 4 байта – протоколу Wiegand-34, 7 байт – протоколу Wiegand-58.
lpNumber	Строка гос. номера автомобиля, полученная от интегрированной системы видеонаблюдения.
empid	Внутренний идентификатор сотрудника в базе «Sigur».
direction	Направление запрошенного доступа: <ul style="list-style-type: none"> <li>1 - выход.</li> <li>2 - вход.</li> <li>3 - неизвестное.</li> </ul>
accessPoint	Номер точки доступа, где произошла идентификация сотрудника. Соответствует номеру точки доступа на вкладке «Оборудование» ПО «Клиент».

В ответ на запрос «Sigur» ожидает получить следующий объект (пример):

```
{
  "allow": false,
  "message": "Недостаточно средств на счете"
}
```

### Содержимое тела ответа внешней системы на HTTP POST-запрос.

Параметр	Значение
allow	Разрешение или запрет доступа: <ul style="list-style-type: none"> <li>false, если доступ нужно запретить.</li> <li>true, если доступ нужно разрешить.</li> </ul>

Параметр	Значение
message	Если «allow» имеет значение «false»: сообщение о причине запрета доступа, которое будет помещено в архив системы и отображено на вкладке «Наблюдение». Если параметр «message» отсутствует или равен пустой строке, то система зафиксирует событие по умолчанию – «Доступ запрещен. По решению внешней системы».

Если параметр «allow» имеет значение «true», то в ответе также могут присутствовать какие-либо из дополнительных полей, указанных в таблице ниже.

**Описание дополнительных параметров в теле ответа от внешней системы.**

Параметр	Значение
reqDPass	Требование приложить вторую карту (доступ по правилу двух лиц): <ul style="list-style-type: none"> <li>false – не требуется.</li> <li>true – требуется.</li> </ul>
reqOpr	Требование санкции охраны на проход: <ul style="list-style-type: none"> <li>false – не требуется.</li> <li>true – требуется.</li> </ul>
reqPin	Требование ввести PIN-код: <ul style="list-style-type: none"> <li>false – не требуется.</li> <li>true – требуется.</li> </ul>
pin	Правильный PIN-код. Целое число. Используется, если reqPin="true".
reqEscort	Требование приложить карту сопровождающего: <ul style="list-style-type: none"> <li>false – не требуется.</li> <li>true – требуется.</li> </ul>
escortRuleId	ID допустимой группы сопровождения. Используется, если reqEscort="true".
escortProb	Вероятность запроса сопровождающего в процентах, число от 0 до 100. Используется, если reqEscort="true"
alkoProb	Провести алкотестирование с указанной вероятностью. Значение должно быть целым числом от 0 до 100.
alkoAllowDrunk	Пропускать людей в состоянии алкогольного опьянения: <ul style="list-style-type: none"> <li>false – не требуется.</li> <li>true – требуется.</li> </ul> Используется, если alkoProb>0.

Параметр	Значение
alkoThr	Пороговая концентрация алкоголя в сотых долях. Используется, если alkoProb>0.
extReaderConf	<p>Политика использования дополнительного считывателя (как правило, картоприёмника):</p> <ul style="list-style-type: none"> <li>▪ DEFAULT – обрабатывать дополнительный считыватель так же, как основной;</li> <li>▪ GUESTREADER – воспринимать дополнительный считыватель как картоприёмник;</li> <li>▪ REGISTRATOR – воспринимать дополнительный считыватель как устройство регистрации прохода в неурочное время;</li> <li>▪ PRIMARYONLY – не пропускать через дополнительный считыватель.</li> </ul>
dReadAction	<p>Действие системы при двойном поднесении карты к считывателю:</p> <ul style="list-style-type: none"> <li>▪ NO_ACTION – не выполнять никаких действий;</li> <li>▪ NORMAL_UNLOCKED – менять режим точки доступа: нормальный &lt;-&gt; разблокированный;</li> <li>▪ NORMAL_LOCKED – менять режим точки доступа: нормальный &lt;-&gt; заблокированный;</li> <li>▪ LOCKED_UNLOCKED – менять режим точки доступа: заблокированный &lt;-&gt; разблокированный.</li> </ul>
itemToSell	ID пункта меню, который необходимо «продать» при проходе. Доступ будет запрещен, если продажа невозможна.
faceVer	<p>Политика верификации лица. Варианты:</p> <ul style="list-style-type: none"> <li>▪ OFF – не проводить верификацию лица.</li> <li>▪ SOFT – провести «мягкую» верификацию (пустить в любом случае).</li> <li>▪ HARD – провести «жесткую» верификацию (пустить только при совпадении лица).</li> </ul>

## 4.2. Доставка проходов

Если в настройках задан URL доставки событий проходов, то при наличии недоставленных проходов «Sigur» выполнит HTTP(S) POST-запрос по указанному URL.

Пример данных, которые могут быть переданы в теле запроса внешней системе:

```
{
  "logs": [
    {
      "logId": 925244,
      "time": 1510826281,
      "empld": "",
      "internalEmpld": 0,
      "accessPoint": 1,
      "direction": 2,
      "keyHex": "5AB860"
    },
    {
      "logId": 925247,
      "time": 1510826858,
      "empld": "",
      "internalEmpld": 0,
      "accessPoint": 1,
      "direction": 2,
      "keyHex": "5AB860"
    }
  ]
}
```

JSON-объект в теле запроса внешней системе всегда содержит поле logs, являющееся массивом проходов.

### Значение параметров массива logs.

Параметр	Значение
logId	Идентификатор события. Целое число. Система гарантирует монотонное увеличение данных идентификаторов, т.е. события, которые стали известны системе позже, будут иметь большее значение идентификатора. Система также гарантирует, что в одном запросе проходы передаются в порядке увеличения значений logId.
time	Время возникновения события. Целое число. Unix time по времени часового пояса, где возникло событие.

Параметр	Значение
empld	ID объекта доступа во внешней системе. Строка. Равно пустой строке, если объект не был ранее загружен из внешней системы.
internalEmpld	ID объекта доступа в базе системы. Целое число. Равно 0, если объект отсутствует в базе системы.
accessPoint	ID точки доступа в системе. Целое число (*).
direction	Направление совершенного прохода: <ul style="list-style-type: none"> <li>1 - выход.</li> <li>2 - вход.</li> <li>3 - неизвестное.</li> </ul> Целое число (*).
keyHex	Номер идентификатора, использованного при проходе и принятого от считывателя на контроллер. Строка (*).

(\*) - данные поля по содержанию соответствуют одноименным полям в запросе на делегирование.

В одном запросе система может передать от 1 до 100 событий прохода.

В ответ на запрос «Sigur» ожидает получить от внешней системы следующий объект (пример):

```
{
  "confirmedLogId": 925247
}
```

**Содержимое тела ответа внешней системы на HTTP POST-запрос.**

Параметр	Значение
confirmedLogId	Идентификатор события, полученный внешней системой в поле logId одного из событий. Получив какое-то значение этого поля, «Sigur» будет считать доставленными во внешнюю систему все события с идентификаторами до полученного включительно.

## 5. Контакты

ООО «Промышленная автоматика – контроль доступа»  
Адрес: 603001, Нижний Новгород, ул. Керченская, д. 13, 4 этаж.

Система контроля и управления доступом «Sigur»

Сайт: [www.sigur.com](http://www.sigur.com)

По общим вопросам: [info@sigur.com](mailto:info@sigur.com)

Техническая поддержка: [support@sigur.com](mailto:support@sigur.com)

Телефон: +7 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260 12 93